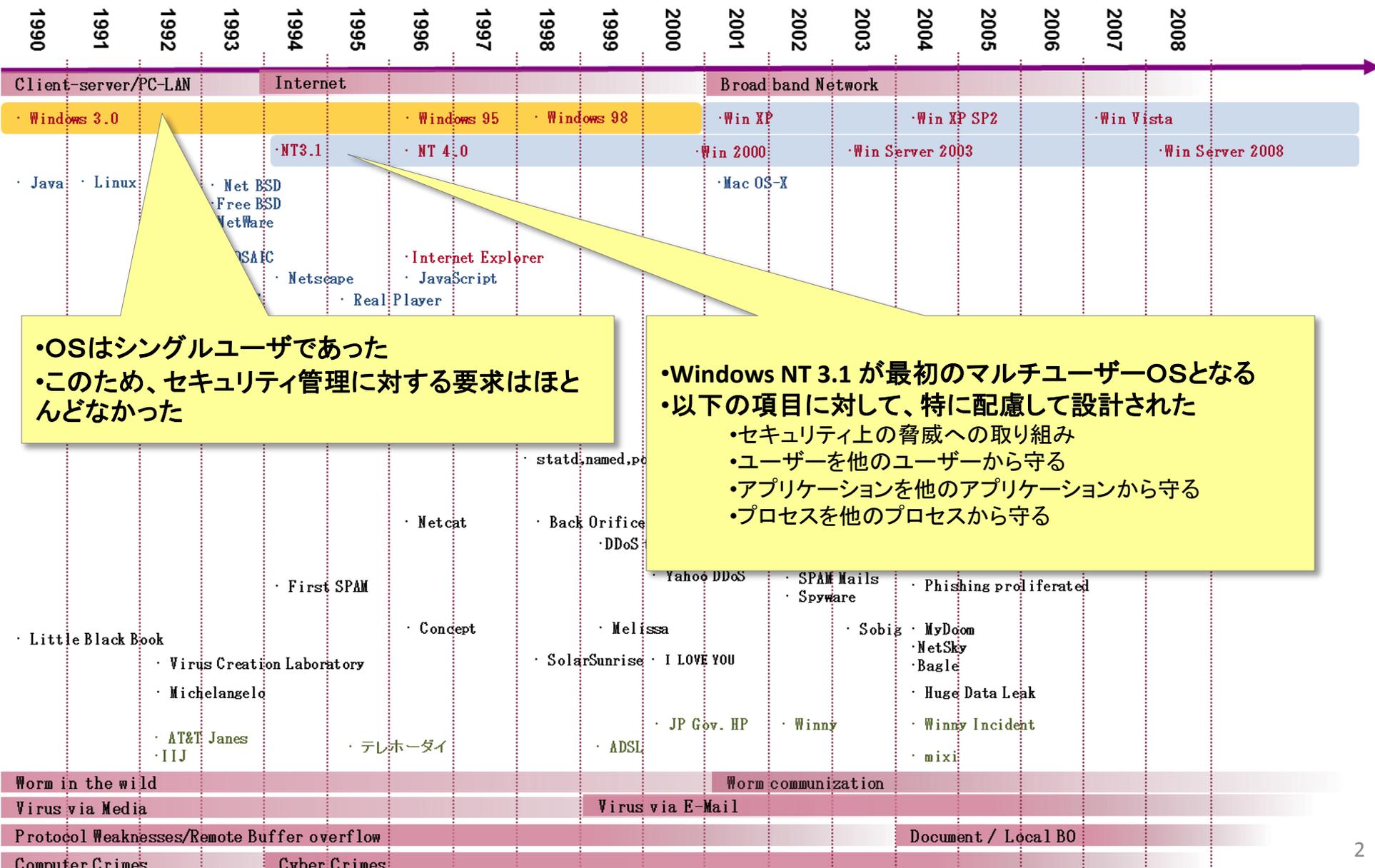


# 脆弱性への取組みーマイクロソフト社の事例 ～いかにしてSDLにたどり着いたのか～

日本マイクロソフト株式会社  
チーフセキュリティアドバイザー  
高橋 正和

# Windows Products and Security

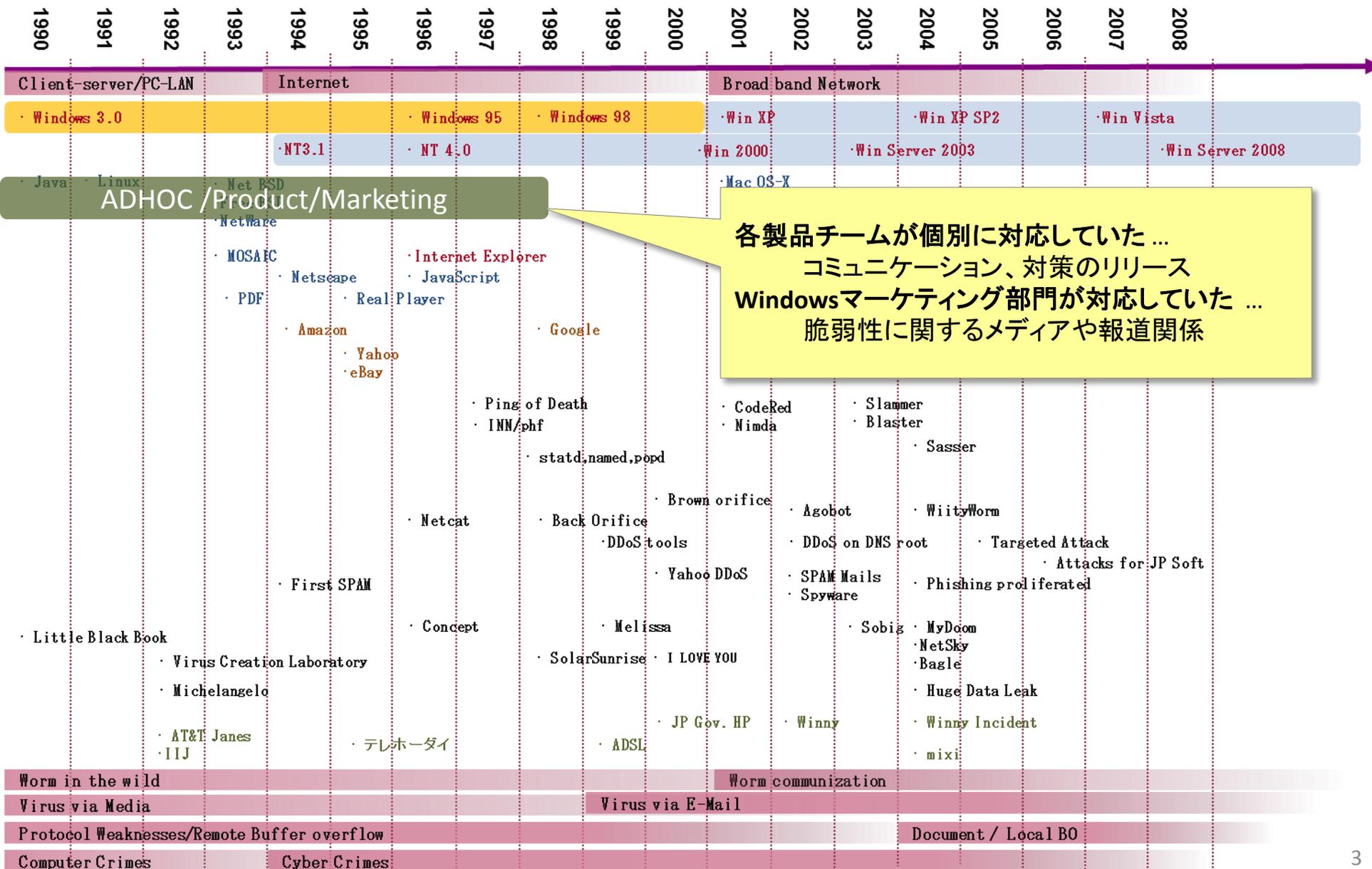


・OSはシングルユーザであった  
 ・このため、セキュリティ管理に対する要求はほとんどなかった

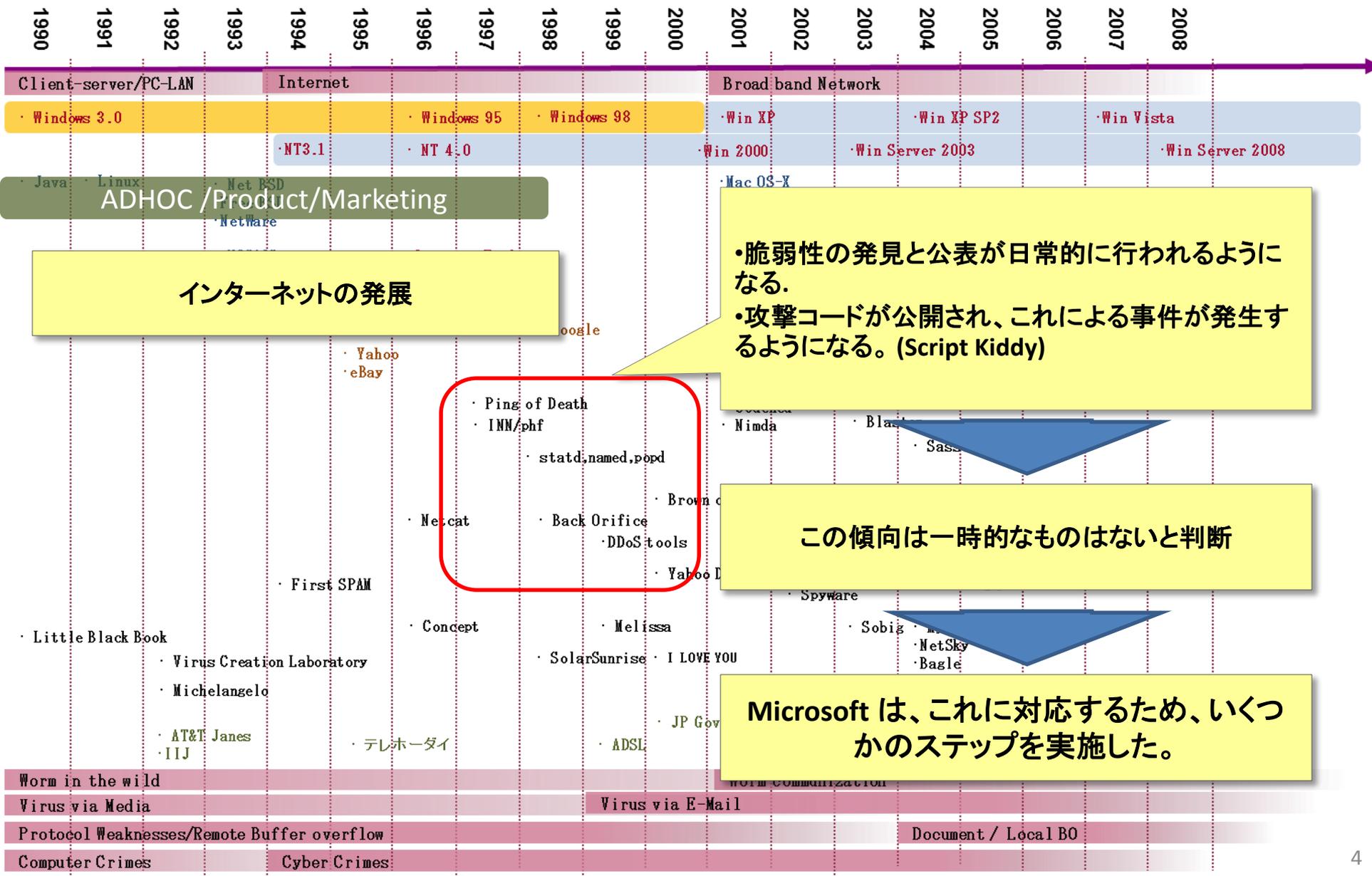
・Windows NT 3.1 が最初のマルチユーザーOSとなる  
 ・以下の項目に対して、特に配慮して設計された

- ・セキュリティ上の脅威への取り組み
- ・ユーザーを他のユーザーから守る
- ・アプリケーションを他のアプリケーションから守る
- ・プロセスを他のプロセスから守る

# Windows Products and Security: 1998年以前



# Windows Products and Security: 1990年代中頃

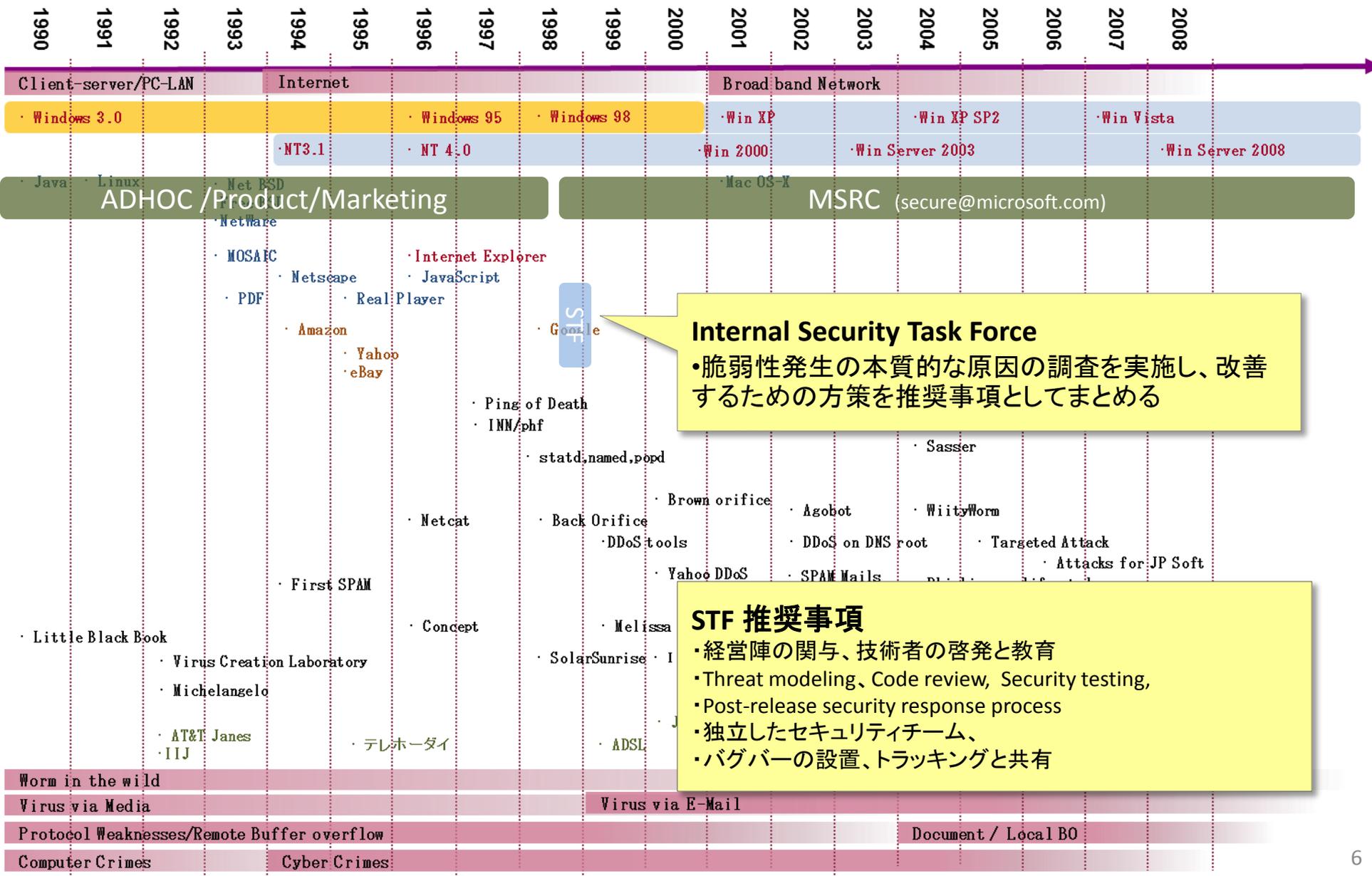


# SANS: 最も重要なインターネット上の脅威

## The Top 10 Most Critical Internet Security Threats (2000-2001)

1	BIND weaknesses: nxd, qinv and in.named allow immediate root compromise.
2	Vulnerable CGI programs and application extensions (e.g., ColdFusion) installed on web servers
3	Remote Procedure Call (RPC) weaknesses in rpc.ttdbserverd (ToolTalk), rpc.cmsd (Calendar Manager), and rpc.statd that allow immediate root compromise
4	RDS security hole in the Microsoft Internet Information Server (IIS)
5	Sendmail and MIME buffer overflows as well as pipe attacks that allow immediate root compromise
6	sadmind and mountd
7	Global file sharing and inappropriate information sharing via NetBIOS and Windows NT ports 135->139 (445 in Windows2000), or UNIX NFS exports on port 2049, or Macintosh Web sharing or AppleShare/IP on ports 80, 427, and 548
8	User IDs, especially root/administrator with no passwords or weak passwords
9	IMAP and POP buffer overflow vulnerabilities or incorrect configuration
10	Default SNMP community strings set to 'public' and 'private.'

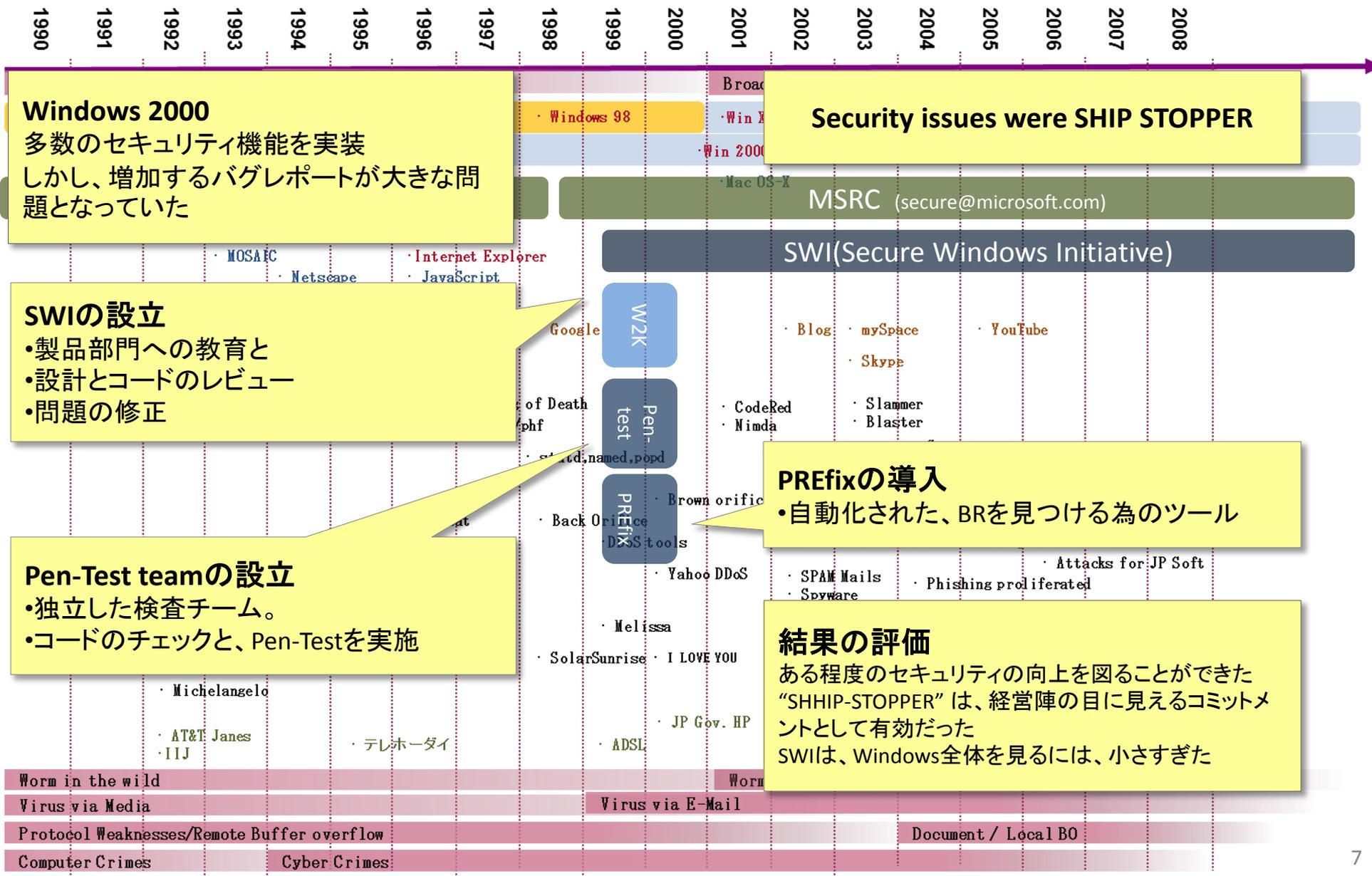
# Windows Products and Security: 最初のステップ



**Internal Security Task Force**  
 •脆弱性発生の本質的な原因の調査を実施し、改善するための方策を推奨事項としてまとめる

**STF 推奨事項**  
 •経営陣の関与、技術者の啓発と教育  
 •Threat modeling、Code review、Security testing、  
 •Post-release security response process  
 •独立したセキュリティチーム、  
 •バグバーの設置、トラッキングと共有

# Windows Products and Security: Windows 2000



**Windows 2000**  
 多数のセキュリティ機能を実装  
 しかし、増加するバグレポートが大きな問題となっていた

**Security issues were SHIP STOPPER**

MSRC (secure@microsoft.com)

SWI(Secure Windows Initiative)

**SWIの設立**  
 ・製品部門への教育と  
 ・設計とコードのレビュー  
 ・問題の修正

**PREFIXの導入**  
 ・自動化された、BRを見つける為のツール

**Pen-Test teamの設立**  
 ・独立した検査チーム。  
 ・コードのチェックと、Pen-Testを実施

**結果の評価**  
 ある程度のセキュリティの向上を図ることができた  
 “SHHIP-STOPPER” は、経営陣の目に見えるコミットメントとして有効だった  
 SWIは、Windows全体を見るには、小さすぎた

Worm in the wild  
 Virus via Media  
 Protocol Weaknesses/Remote Buffer overflow  
 Computer Crimes  
 Cyber Crimes  
 Virus via E-Mail  
 Document / Local BO

# Windows Products and Security: Windows XP

1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008

## Windows XP

さらなる、効果的な取り組みが必要とされた security.

## 確実なセキュリティの向上のため...

- 技術者の支援を中心に移行
- 魚(脆弱性)を釣る代わりに、魚の釣り方を教える
- “Security Days” “bug bashes”: これを、確実に実施するための施策

## Security Day / Bug bash

2~4時間のセキュリティトレーニングで始まり、その日の復習で終了する。  
 コードのレビューを行い、ペネトレーションテスト(侵入テスト)や、その他のセキュリティテストを指導する。する、  
 “最高のセキュリティバグ賞”等を設置し、表彰を行う。

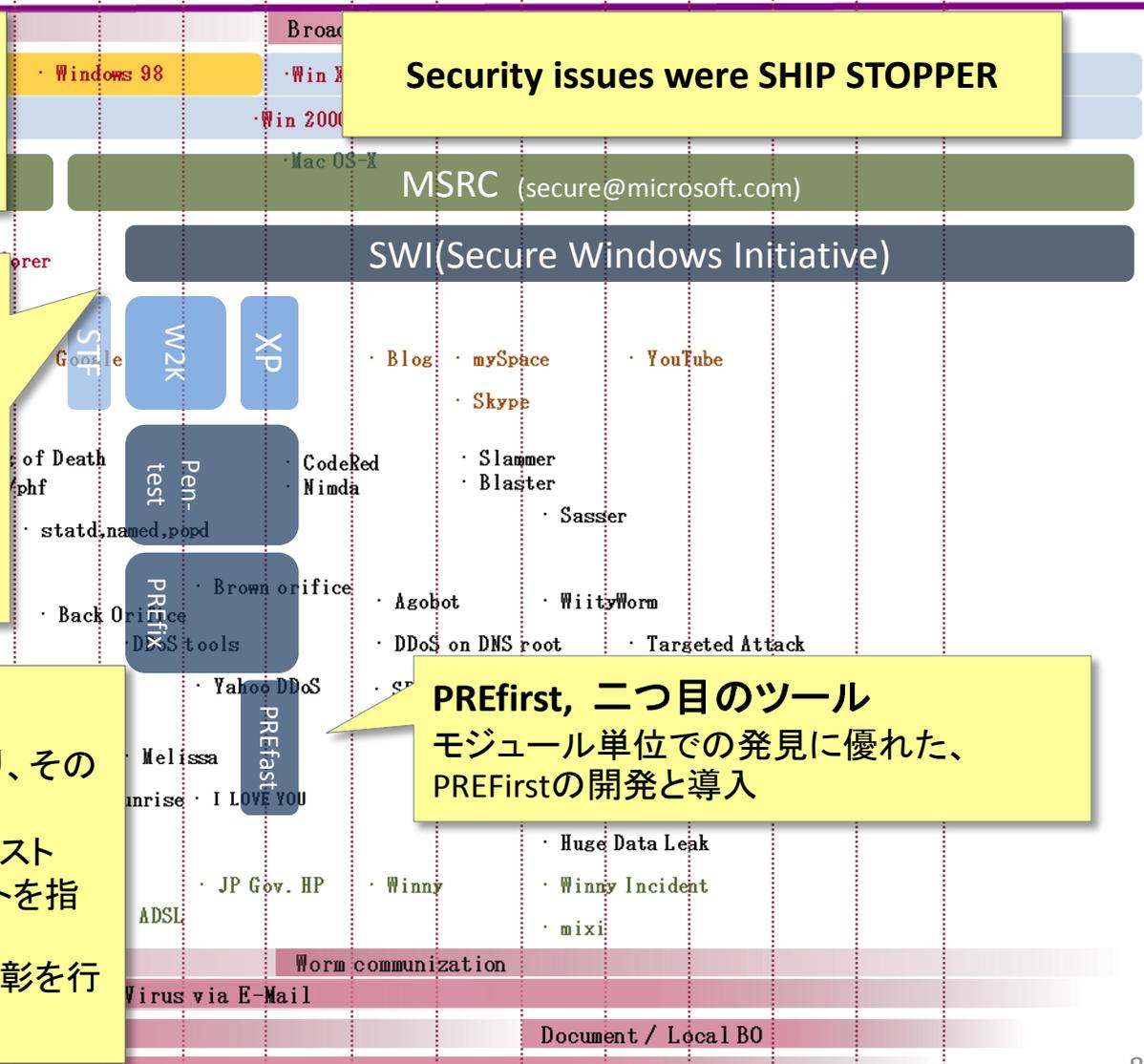
## Security issues were SHIP STOPPER

MSRC (secure@microsoft.com)

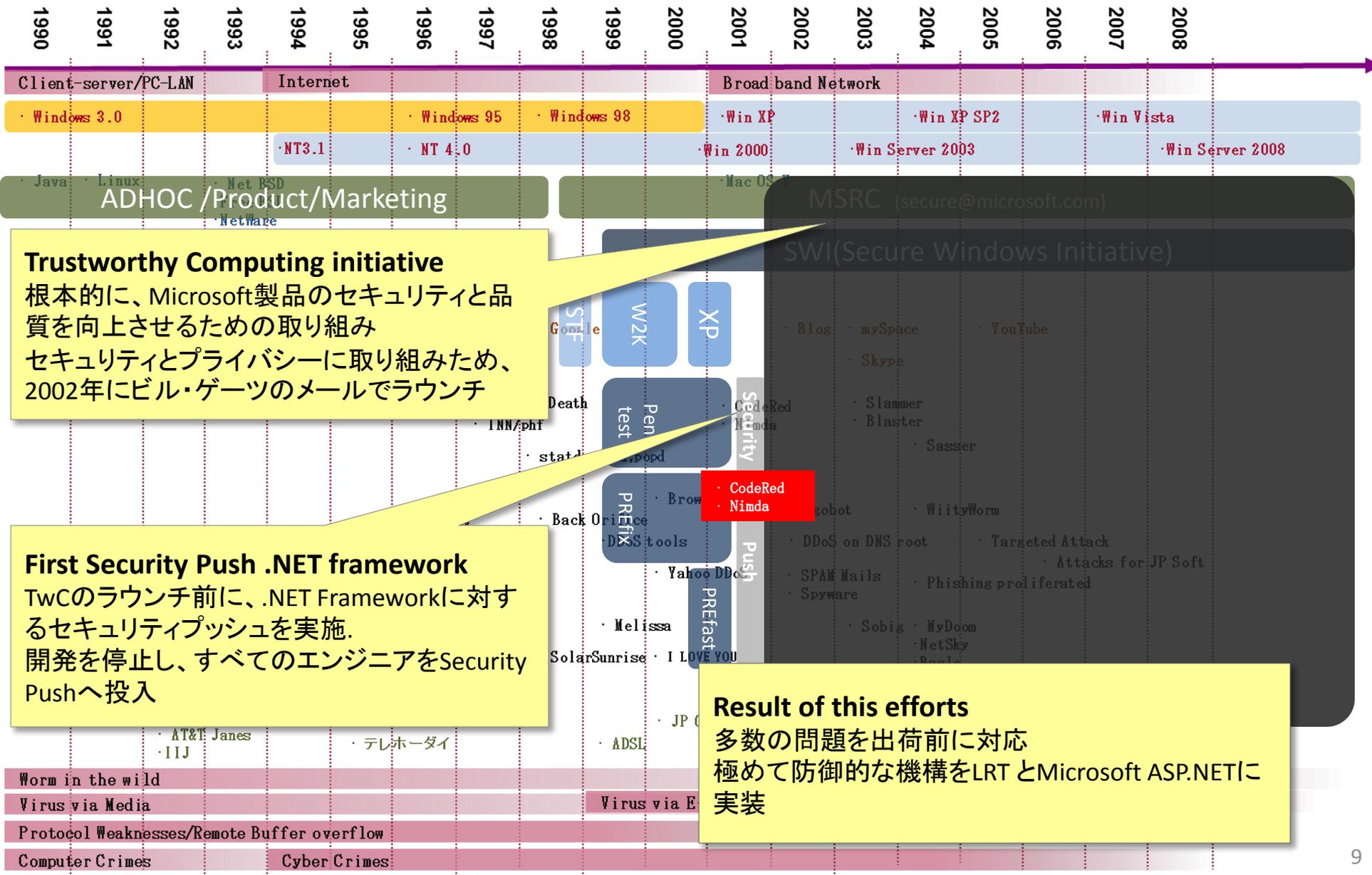
## SWI(Secure Windows Initiative)

## PREfirst, 二つ目のツール

モジュール単位での発見に優れた、PREFirstの開発と導入



# Windows Products and Security: Windows XP

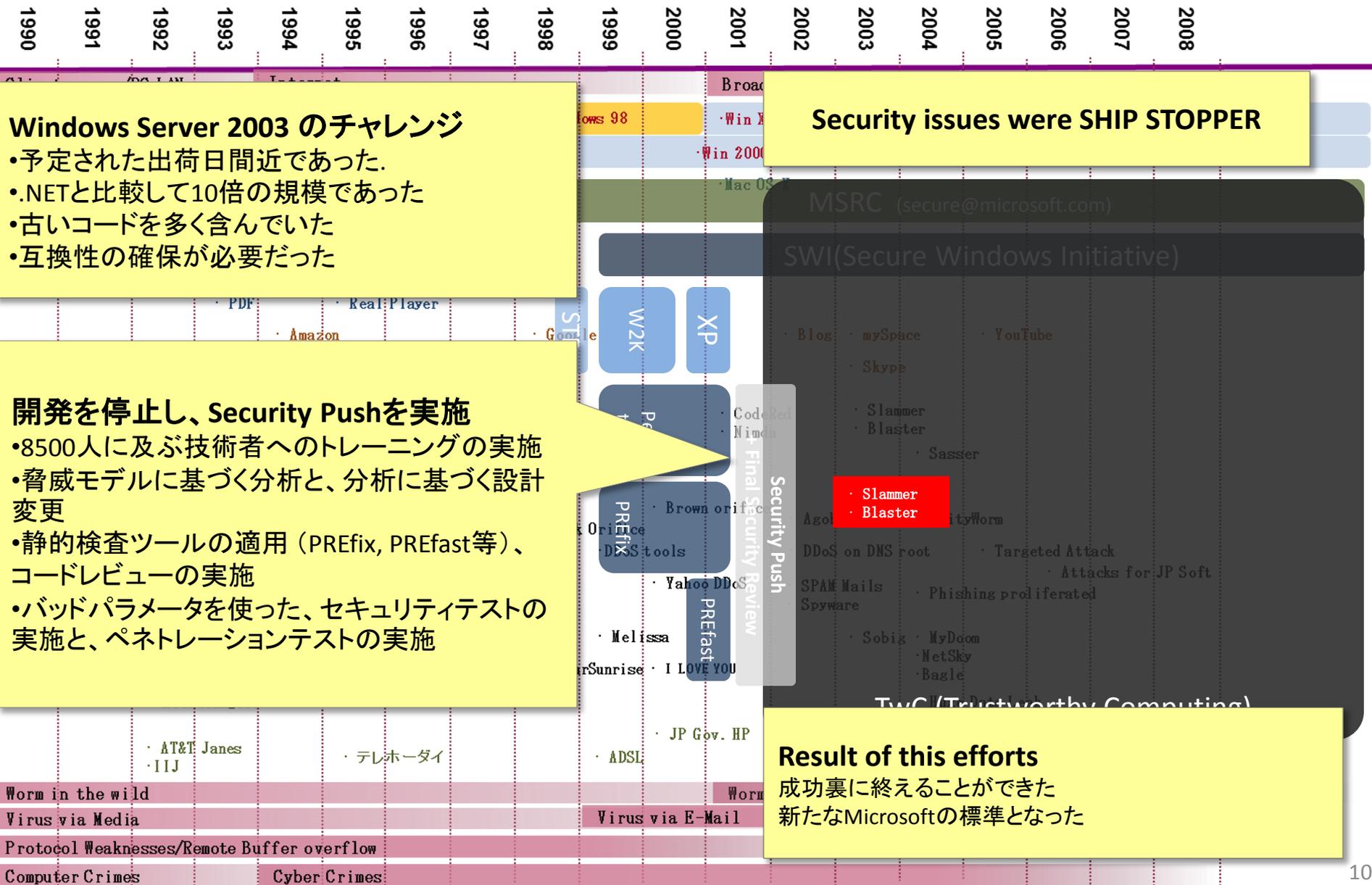


**Trustworthy Computing initiative**  
 根本的に、Microsoft製品のセキュリティと品質を向上させるための取り組み  
 セキュリティとプライバシーに取り組みため、2002年にビル・ゲーツのメールでラウンチ

**First Security Push .NET framework**  
 TwCのラウンチ前に、.NET Frameworkに対するセキュリティプッシュを実施。  
 開発を停止し、すべてのエンジニアをSecurity Pushへ投入

**Result of this efforts**  
 多数の問題を出荷前に対応  
 極めて防御的な機構をLRTとMicrosoft ASP.NETに実装

# Windows Products and Security: Windows XP



## Windows Server 2003 のチャレンジ

- 予定された出荷日間近であった。
- .NETと比較して10倍の規模であった
- 古いコードを多く含んでいた
- 互換性の確保が必要だった

## Security issues were SHIP STOPPER

## 開発を停止し、Security Pushを実施

- 8500人に及ぶ技術者へのトレーニングの実施
- 脅威モデルに基づく分析と、分析に基づく設計変更
- 静的検査ツールの適用 (PREfix, PREfast等)、コードレビューの実施
- バッドパラメータを使った、セキュリティテストの実施と、ペネトレーションテストの実施

MSRC (secure@microsoft.com)

SWI(Secure Windows Initiative)

Blog · mySpace · YouTube

Skype

Slammer · Blaster

Sasser

Agobot · Nimda · Worm

DDoS on DNS root · Targeted Attack

SPAM Mails · Phishing proliferated

Spyware

Sobig · MyDoom

NetSky

Bagle

TWC (Trustworthy Computing)

## Result of this efforts

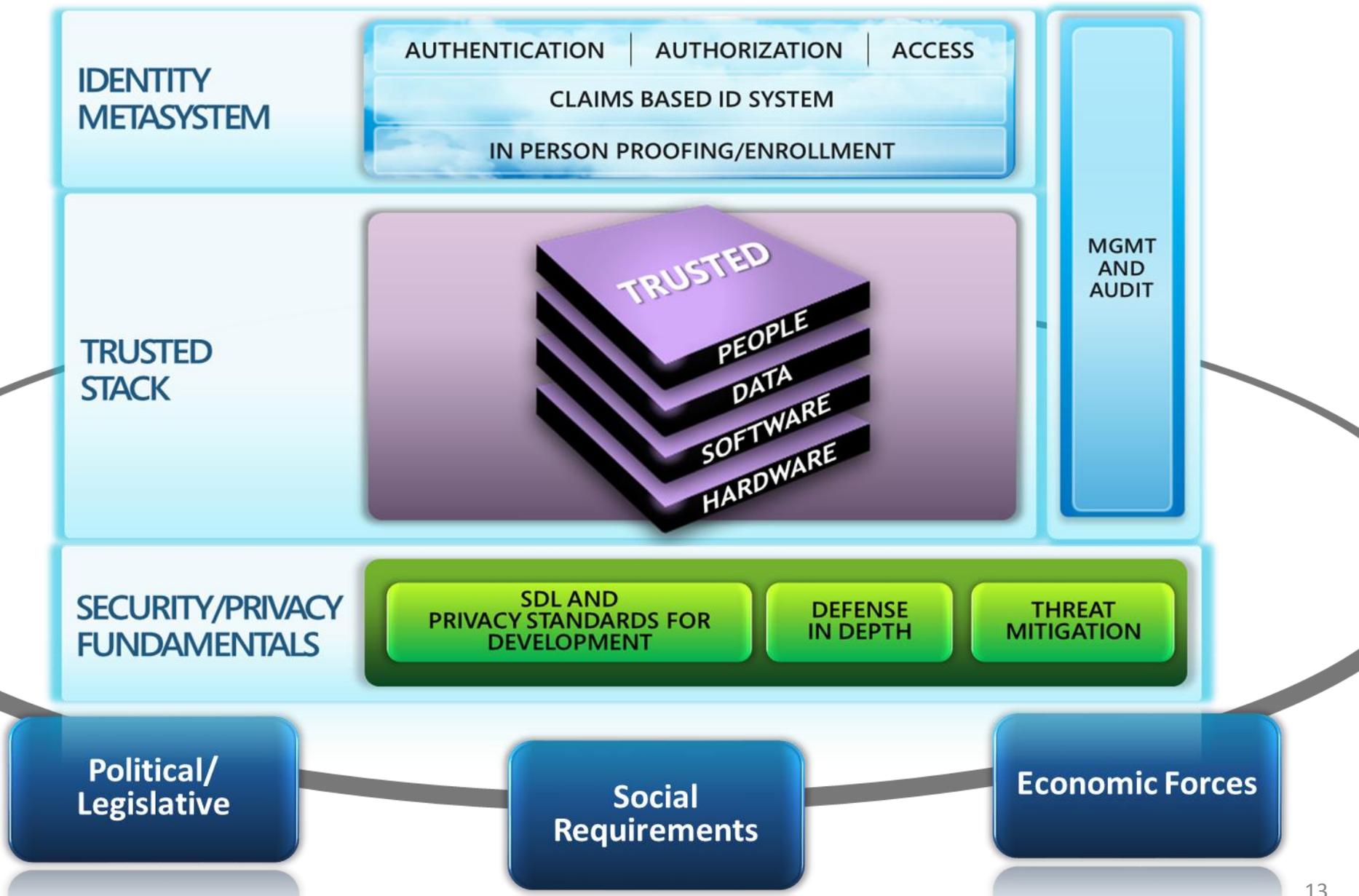
成功裏に終わることができた  
新たなMicrosoftの標準となった



# SDLに関して学んだこと

- セキュリティテストは、重要な要素だが、十分ではない
- セキュアコーディングは、重要な要素だが、十分ではない
- 脅威分析は、重要な要素だが、十分ではない
- エンジニアの啓発とトレーニングは、重要な要素だが、十分ではない
- 経営陣のコミットメントは重要な要素だが、十分ではない
  - これらのすべては、個別に実施していたのでは効果的ではない
- 必要とされる要素を、効果的かつ安定したエンジニアリングとしてプロセスとする必要がある。
  - 具体的な手法については、最初のページ “**Security Development Lifecycle Overview**” を見てください

# End to End Trust: 新たなセキュリティモデル



# 最後に

- 思わぬ形で、ITが利用されている
  - ネットワークや端末、コントロールサーバーとして
    - もしかして、PCが端末になっていませんか？
    - もしかして、ブラウザで制御してませんか？
    - もしかして、TCP/IPとか使ってませんか？
      - ロボットのカタログを見ると、RJ45のインタフェースがついていることが多い
    - もしかして、、、
- アンダーグラウンドビジネス
  - 絵空事だと思われるでしょうが。。。
    - 「すべてに価値がある」= 売買が可能である
      - クレジットカードなどの換金請負、ブランクカード、エンボスの販売
      - ロンダリング用のアカウントの提供者
      - 再配送サービス
      - 暗号解読サービス(4時間で38%が解読可能だったらしい)
  - 組み込み機器もハックされている
    - モチベーションの問題



© 2012 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.